Regulatory Compliance.

Operations and Systems Outsourcing: Compliance Considerations for Broker-Dealers.

Broadridge®

Introduction

Due to the efficiencies and economics of outsourcing, broker-dealers are relying more and more on outsourcing for a variety of tasks. However, because of new and stricter regulations, outsourcing presents ever-growing compliance and oversight challenges.

THE NEXT WAVE OF NEW REGULATIONS IS EXPECTED THIS YEAR.

Regulators have consistently stated that while firms may outsource many types of activities and processes, the firms themselves remain ultimately responsible for oversight and compliance with securities laws, stock exchange rules and other SRO regulations. Recently, FINRA proposed new rules on outsourcing, and the agency's enforcement arm has already demonstrated that it will hold broker-dealers accountable for failures resulting from activities carried out by vendors, most recently in the area of prospectus delivery. Further evidence of the importance of this topic is illustrated by FINRA's January 2012 publication of its annual regulatory and examination priorities, which included outsourcing as a key risk and concern. [1]

This white paper describes trends in compliance regulation of broker-dealer outsourcing and suggests how firms can best prepare to meet these standards.

IN THIS PAPER, WE WILL:

- Examine current outsourcing trends and how they impact the broker-dealer community
- Describe new legal and accounting standards and offer strategies for compliance
- Discuss recent enforcement actions and inspections, what this means for broker-dealers and how technology can help provide solutions
- Outline ten best practices and provide tips for managing relationships with your third-party vendors

[1] Available at http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p125492.pdf.

Today's Increasingly Outsourced World

The benefits of outsourcing are easy to see—outsourcing to vendors with specific expertise is efficient and can save both time and money without necessarily sacrificing responsiveness or excellence in customer service.

This solution is especially important at a time when brokers' service offerings are expanding. On the most basic level, outsourcing frees internal employees to focus on other pressing business needs. Plus, it offers flexibility to bring in an expert when there is no infrastructure to do so internally, or when services are only needed temporarily. In a broader sense, outsiders bring not only their skills but also a new perspective to the table.

A NYSE and NASD (now FINRA) study completed a number of years ago found that broker-dealers frequently outsource functions associated with accounting and finance (payroll, expense account reporting, etc.), legal and compliance, information technology (IT), operations functions (e.g., statement production, disaster recovery services, etc.) and administration functions (e.g., human resources, internal audits, etc.). At the time of this landmark study, most respondent broker-dealers had not implemented written outsourcing compliance or due diligence procedures.

The survey results spurred a first wave of regulatory attention, and a number of new outsourcing guidelines were implemented shortly thereafter. In 2005, FINRA published outsourcing guidance in Notice to Members 05-48. Notably, it mandated that parties conducting activities that require registration under the FINRA rules will be considered "associated persons" of the member, and that outsourcing does not relieve members of their ultimate compliance responsibilities.

As technological capabilities advanced, outsourcing continued to expand. FINRA received an increasing number of inquiries regarding the scope and specifics of the guidance provided by NT 05-48, spurring yet more regulatory action. At the same time, there was pressure to update audit standards to deal with increasingly global outsourcing and a wider audience, including not only auditors but also executives.

> **"While firms may contract with outside vendors for the provision of securities related services, compliance with the federal securities laws and NYSE rules is the sole responsibility of the firms and may not be assigned or delegated to others."**
>
> **— New York Stock Exchange Regulation Press Release, October 8, 2007[2]**

[2] Available at http://www.nyse.com/press/1191838488330.html.

MORE STRINGENT REGULATORY REQUIREMENTS AND INSPECTIONS

In March 2011, FINRA proposed Rule 3190, reaffirming the agency's existing mandate that a firm may not outsource its ultimate responsibility for oversight and compliance. It also added more specifics to the previous guidance.

Under the proposed rule, a firm must:

- Maintain a supervisory system and written procedures for any functions performed by a third party that are designed to ensure compliance
- Conduct ongoing due diligence to ensure the third party is capable of performing the functions in a compliant manner

Rule 3190 is currently expected to be adopted in the first half of 2012. In conducting inspections, FINRA is likely to apply increased scrutiny, particularly after the proposed rule is adopted. Within a year or so following adoption, it would not be surprising if there were a series of enforcement actions based on the new rule.

STEPPED-UP INSPECTIONS, ENFORCEMENT AND THE ROLE OF TECHNOLOGY

There is plenty of proof pointing to firms being held accountable for their outsourced activities. NYSE Regulation (now part of FINRA) has previously brought actions for prospectus delivery failures against firms that outsourced the documents' delivery and fell short of specified requirements. Evidence reveals that in some cases third-party service providers had asked for instructions on how to handle delinquent prospectuses but did not receive an adequate response. This is yet another indication that the broker-dealer must always treat compliance with the same level of diligence as if it were being done in-house.

In the past, a broker-dealer or its service provider was required to maintain a physical supply of prospectuses to ensure that a client would receive the appropriate document in compliance with regulatory requirements. However, mutual fund companies would often fail to supply the broker or service provider with an adequate supply, leading to delinquencies.

Today, technology benefits brokers in this area with services such as Print on Demand which, when coupled with regulatory approval of summary prospectuses, has made staying in compliance easier and more cost effective.

However, technological advancements have also increased the demands on broker-dealers; regulators can more easily demand more information and faster responses. Regulations are likely to continue to move in this direction, as technology grows faster and more sophisticated, and the ability to access and transmit information continues to grow.

FINRA CONTINUES TO ESCALATE ENFORCEMENT OF REGULATIONS WITH SERIOUS CONSEQUENCES

In 2010, FINRA filed 13% more enforcement actions than in the previous year (although it is estimated that total fines were down slightly for this time). Through December 16, 2011, in an overall increase since 2010, FINRA had brought 1,411 disciplinary actions against registered individuals and firms, levied fines of greater than $63 million and ordered more than $19 million in restitution to investors. In this time, FINRA also expelled 17 firms from the securities industry, barred 317 individuals and suspended 432 brokers from association with FINRA-regulated firms.[3]

NEW ACCOUNTING STANDARDS REFLECT THE NEW REGULATORY ENVIRONMENT

Reflecting the new focus on outsourcing and compliance, additional auditing standards have been issued to assist firms in supervising third party vendors, among other reasons. In June of this year, SAS 70, the former standard for auditing service organizations, was replaced with two new standards: SSAE No. 16 and ISAE 3402.

The new standards are not only tailored to fit outsourcing in today's global business environment, but are in many ways more rigorous than the previous standard, looking at regulatory, compliance, operational and disaster recovery controls. For example, in regard to proxy processing, the new standards provide for several different levels of attestation—of varying degrees of toughness—that evaluate design, implementation, suitability and operating effectiveness of controls. The most stringent SSAE No. 16 attestation—a Statement of Control (SOC) 1, Type II attestation—also includes a financial component, reviewing and testing billing and other financial variables for the entire period under review.

One of the biggest challenges management now faces is that it must provide a written assertion (based on internal and external audit reports and their own monitoring activities) regarding its control system. Detail of the control system's design and objectives, as well as success in facing identified risks, is required. Management also must describe any non-compliance with legal standards and control design deficiencies and failures.

[3] See http://www.finra.org/Newsroom/NewsReleases/2011/P125263.

Best Practices

We interviewed several firms—both regional and national—regarding their compliance practices. The following are some key best-practice takeaways from our interviews. These practices need to be tailored and scaled to each individual firm, taking into account its size, location and other factors.

1

Treat all outsourced activity with the same standards that you would use in-house.

Treat outsourced activities as if you were still doing them in-house. Keep in regular contact with the vendor, engage them on current transactions or problems, and ideally, make on-site visits. Every firm should review activity reports that vendors generate and promptly respond to any red flags. If your vendor does not generate reports, ask them to. One large firm conducts quarterly review meetings with its proxy vendor, coupled with weekly calls and periodic site visits to address specific issues.

Find out if your vendor makes online portals available to monitor "real-time" transactions in your account. If so, take advantage of that resource to periodically monitor transactions.

2

Leverage new technology to help you stay in compliance.

Technology provides a means to enhance your vendor's ability to remain in compliance. As an example, technology can permit a firm to monitor proxy delivery processes or operations in real-time. Confirm that your vendor can provide the expertise and innovative technology to help you efficiently manage your obligations. Intelligent technology should have the scale, capacity and infrastructure to ensure compliance, while simultaneously saving you time and money. When considering your own capabilities, make certain you have adequate checks and balances to identify all transactions that require service on the part of your third-party vendors.

3

Carefully research any new vendor's reputation before deciding to use its services.

Your vendor's standing can either help or harm your own reputation. In selecting a third party, consider the vendor's own reputation, track record and experience in dealing with the types and volumes of transactions that are part of the relationship.

Consider how the vendor stacks up against the rest of the market. Make an effort to speak to your potential vendor's past and current clients and, if possible, clients of competitors as well.

4

Identify unique situations you could leverage to trigger audits, and don't be afraid to dig into your vendor's work.

Constantly review your vendor's work in a way that makes sense for your firm. For example, one firm uses client inquiries or complaints, such as late receipt of a proxy statement, to trigger probes for accuracy. On the prospectus delivery side, another audits mail returned to the broker to verify the contents, mailing dates and other information. Another tactic on the prospectus side is to ask for specific cusip numbers to be pulled during site visits, checking to see that the correct documents are on file. While not as helpful in cases of high mailing volumes, some firms might pull random samples from a mailing and check for accuracy and completeness, or even audit each and every transaction.

5

Know your vendor's compliance controls then review audits and other compliance documents.

In most cases, you should insist on appropriate audits of the vendor's operations. SSAE No. 16, noted above, includes several attestation standards, ranging from the least stringent Statement of Control 3, a snapshot of controls, to the most stringent SOC 1 Type II, reporting on controls and financial information over a period of time. What attestation standard does your vendor use? Does this provide sufficient information to reliably evaluate all relevant controls over time?

The new standards do not require critical judgment by an auditor—meaning that end-users must evaluate the contents of the report. Does management's letter identify controls and risks that are important to you? Does the report reflect any "exceptions" or control failures and, if so, has management taken sufficient action to remediate problems and assure future compliance?

6

Familiarize yourself with your vendor's legal compliance reviews, then review the results.

Your vendor should be subject to multiple internal and external checks and balances—such as both internal and external audits and other compliance reviews—each focusing on different priorities or looking at the organization from different angles. This is done in order to ensure that your processes are being performed as expected.

Insist on other legal compliance reviews and other self-evaluation procedures that are appropriate for your vendor's business. Review and understand all legal compliance reports provided by your vendor, and make sure you understand any problems highlighted and how they are being corrected. Consider if your vendor is conducting internal audits, and ask to review the results of those analyses.

7

Discuss your vendor's data management and security policies and processes.

Chances are that any vendor performing a critical function has access to confidential financial records. Discuss with your vendor its process for controlling access to data, as well as its process for data monitoring and alerts and reporting of security breaches. The International Standard for Organization (ISO) has developed standards for certification and requirements for the quality of management systems to ensure that they meet the needs of customers and others. Ask if your vendor is ISO-certified, especially in the areas of information security, and remain aware of any changes in certification status throughout your relationship. Consider requiring your vendor to notify you in writing if its ISO status changes.

8

Know your vendor's disaster management and recovery plans, as well as your own emergency back-up plans.

Know and understand what your vendor plans to do in case of emergency, be it a technology problem, a natural disaster that affects your business or a data security breach. Understand and document your own back-up plans, including plans in cases where your vendor's services are no longer available. ISO certification also covers a vendor's disaster recovery plans and process, stressing the importance of being aware of your vendor's certification status.

9

Aid each vendor in creating service benchmarks, then review their SLAs.

SLAs allow you to nail down a concrete benchmark against which to judge a vendor's performance. Tasks, compliance protocol and specific procedures are agreed upon in advance, allowing you to feel comfortable that your vendor understands your expectations. The vendor's compliance with the terms of the agreement should be a part of your regular follow-up communications, including procedures for redressing any deviations.

10

Maintain meticulously detailed records to adequately protect yourself in case of inquiry or investigation.

Keep detailed records of not only your policy for oversight, but also your implementation of that policy. Good records can help detect patterns of issues and track changes in service or quality over time. Plus, they provide a basis for discussions with your vendor about their work. It's also imperative to have complete records to comply with regulatory requirements and you may be asked to produce them in case of a regulatory investigation or inquiry.

With roots that go back more than 40 years, Broadridge is the financial services industry's leading provider of innovative technological and outsourcing services.

Our expertise encompasses every aspect of securities processing and investor communications. Our clients include global banks; retail, institutional and discount brokerage firms; correspondent clearing firms; mutual and hedge funds; investment management organizations; and corporate issuers, all of whom have one thing in common: they look to Broadridge for solutions that help them enhance their performance, increase efficiency, reduce cost and maintain focus on serving clients and shareholders.

For more information about Broadridge's products and solutions, please contact your account manager at broadridgeinfo@broadridge.com.

Broadridge holds the following audits and certifications:
SAS70 Type II and SSAE 16 audits to report on compliance with proper security controls
ISO 9001:2008 Certificate for quality management systems and processes
ISO 27001 Internationally recognized certification for Information and Security Management Systems

Broadridge®